

REMARKS

Reconsideration of this Application is respectfully requested. Applicants wish to thank the Examiner for his kind assistance during the Examiner Interview of this date. Independent claims 1, 14 and 23 are amended pursuant to the Interview, without prejudice or disclaimer, to better define the invention without limiting effect. Claims 1-17, 19, 20, 22 and 23 are in this case.

Initially, in response to Applicants' amendments and arguments as set forth in the Amendment dated September 15, 2004, the Examiner states that he has rejected claims 1, 14 and 23 under 35 U.S.C. § 112, second paragraph, for indefiniteness. In particular, the Examiner indicates a lack of antecedent basis (i.e., "the number of tokens") in the case where N, the number of additional transmissions, is equal to zero. In the amended claims 1, 14 and 23, the Examiner asserts, Applicants' recite "at least one token". He indicates that a better recitation is, perhaps, transmitting "N unique tokens and a checksum...where N is a positive number and defines the number of additional transmissions until another set of tokens is required". The Examiner continues that if $N=0$, then there are no additional transmissions and the other limitations that depend on an at least second transmission do not occur.

More particularly, the Examiner rejected claims 1-17, 19, 20, 22 and 23 under 35 U.S.C. § 112, first paragraph, for allegedly failing to comply with the written description requirement. Specifically, the Examiner takes the position that, while claims 1, 14 and 23 recite the transmission of a "selected value of N", the claim also recites the limitation of "the number of tokens being set to a variable N". The Examiner explains that to one of ordinary skill the term "selected value of N" means a client transmitting to a server a "subset" of the N

number of tokens. The Specification, however, according to the Examiner, recites a client informing a server the value of N and transmitting N tokens for future authentication (Specification, amended page 28). The Examiner notes that claims 2-13 and 15-19, 20 and 22 are rejected as they depend from claims 1 and 14, respectively.

The Examiner also rejected claims 1-17, 19, 20, 22 and 23 under 35 U.S.C. § 112, second paragraph, for indefiniteness. More particularly, the Examiner asserts that claims 1, 14 and 23 recite a variable N that defines the additional number of transmissions used to authenticate a user. However, says the Examiner, if $N=0$, then there are no additional transactions and Applicants' system does not perform, as claimed. He notes that claims 2-13 and 15-19, 20 and 22 are similarly rejected as they depend from claims 1, 14 or 23. The Examiner reiterates his rejection indicated above that claims 1 and 23 are rejected for lack of antecedent basis as to the limitation "the number of tokens" in line 9, and that claims 2-13 are also rejected as they depend from claim 1.

* * * * *

Next, the Examiner rejected claims 1-17, 19, 20 and 22 under 35 U.S.C. § 103(a) as being obvious and, therefore, unpatentable over Pickett, U.S. Patent No. 6,012,144. According to the Examiner, Pickett teaches a transaction security method and apparatus comprising the following steps: (i) transmitting a token to a receiver during first secure transmission between a sender and receiver (Abstract; Figure 4; and column 3, lines 50-52); (ii) establishing at least one additional transmission between the sender and receiver for transmitting the token, wherein the additional transmission is variable and adaptively selected (Figures 4 and 5; column 3, lines 50-54; and column 6, lines 22-35); (iii) comparing

the tokens received during the transmission to establish authenticity (Figures 4 and 5; column 6, lines 23-35 and 64-67); (iv) wherein the at least one token comprises and corresponds to a preselected number of tokens sent during a first secure transmission (Figures 4 and 5); (v) conducting transmissions over unsecure or open connections (Figure 1); (vi) conducting an encrypted first secure transmission (Figures 3A-4; column 5, line 1 through column 6, line 23); (vii) additional transmissions that are sent in plaintext (Figures 1 and 5; column 6, lines 22-35); and (viii) transmitting an acknowledgement from the server to the client upon successful receipt and processing of the first transmission by the client (Column 4, lines 4-14).

The Examiner also indicates that Pickett teaches a sender computer transmitting to a receiver computer a selected value of N and N number of tokens to be used to authenticate the sender computer (Figures 4 and 5) as, for the case of $N=1$, the user “informs” the server of the value of N by registering at least one token to be used for future purchases.

With specific regard to claims 12, 13, 16 and 17, the Examiner takes the position that Pickett additionally teaches transmitting data electronically (citing Figures 1-5). The Examiner then takes Official Notice that checksums are well known computational tools for detecting the presence of errors when data is transmitted over a network. He concludes that it would, therefore, have been obvious to one of ordinary skill to use “checksums” to detect errors during the transmission of sensitive data such as credit card numbers.

As for claims 4, 5 and 22, the Examiner asserts, Pickett further teaches a secure transaction method that comprises multiple transmissions and the exchange of token data (Figures 4 and 5). The Examiner admits that Pickett does not specify a particular number of

additional transmissions. However, he determines, it would have been obvious for a user to register multiple cards but only make one purchase using the service of Pickett, or register one card and make multiple purchases using the one card. Similarly, says the Examiner, as the number of additional transactions of the Pickett system is variable, the number can be ascertained mathematically (i.e., deterministically), or at least statistically, or probabilistically. Moreover, the Examiner states that the choice of independent variables used to model the behavior of said variable is at the discretion of the practitioner.

Last, with respect to claims 19 and 20, the Examiner finds that Pickett teaches a secure transaction method which comprises additional transmissions to a client (Figure 5). With regard to the number of additional transmissions, the Examiner asserts that it would have been obvious for a user to decline using the system of Pickett, or at least a particular website (i.e., ABC Toy Company), (Figure 5) in the future if the user was dissatisfied with the service.

* * * * *

Finally, the Examiner rejected claim 23 under 35 U.S.C. § 103(a) as being obvious and, therefore, unpatentable over Pickett in view of Maher, U.S. Patent No. 6,125,349. According to the Examiner, Pickett teaches a method and system for authenticating transferred data between a sender computer and a receiver computer comprising the following steps: (i) transmitting a token to a receiver during first secure transmission between a sender and receiver (Abstract; Figure 4; and column 3, lines 50-52); (ii) establishing at least one additional transmission between the sender and receiver for transmitting the token, wherein the additional transmission is variable and adaptively selected (Figures 4 and 5;

column 3, lines 50-54; and column 6, lines 22-35); (iii) comparing the tokens received during the transmissions to establish authenticity (Figures 4 and 5; column 6, lines 23-35 and 64-67); and (iv) wherein the at least one token comprises and corresponds to a preselected number of tokens sent during a first secure transmission (Figures 4 and 5).

The Examiner indicates, in addition, that Pickett teaches a sender computer transmitting to a receiver computer a selected value of N and N number of tokens to be used to authenticate the sender computer (Figures 4 and 5). The Examiner acknowledges that Pickett does not explicitly recite specific criteria as input in an algorithm to determine the number of additional transmissions. He then looks to Maher which, he says, teaches a system for authenticating transferred data between a sender computer and receiver computer that uses an algorithm to determine additional transmissions based on frequency of transmissions between sender and receiver, proximity of the sender computer to the receiver computer or usage pattern of the sender (column 6, lines 25-48; column 7, lines 5-25). The Examiner concludes that it would have been obvious to one of ordinary skill to combine the teachings of Pickett and Maher in order to increase usage of the system through a rewards program (column 7, lines 5-25).

* * * * *

First, pursuant to the Examiner Interview, claims 1, 14 and 23 are amended to better define the invention without limiting effect, namely, to clarify (i) a step of “assigning a value [or preselected value] to a variable N where the value of N is a positive number and defines a selected number of additional transmissions”, (ii) that the step of transmitting selected authentication information, “each of the N number of tokens being a unique identifier”, (iii)

that the “N [number of] token(s)” transmitted from the sender [client] computer during the additional transmission is/are compared, (iv) to clarify a step of “assigning a second value to the variable N where the second value of N is a positive number and defines a second selected number of additional transmissions”, and (v) to clarify a step of “transmitting the second value of N, a second value of N number of tokens, and a second checksum value to be used to authenticate the sender computer, from the sender [client] computer to the receiver computer [server], each of the second N number of tokens being a unique identifier”.

Based on the foregoing, withdrawal of the Examiner’s rejections under § 112, first and second paragraphs, is respectfully requested.

As for the rejections under § 103(a), Applicants’ arguments as set forth in the Amendment dated September 10, 2004 are incorporated herein by reference. We respectfully submit that neither Pickett nor Maher, whether taken alone or in any combination, disclose or suggest Applicants’ authentication steps, a variable N as defined, nor the client computer usage patterns, as claimed by Applicants.

Accordingly, withdrawal of the Examiner’s rejections under § 103(a) is also requested.

* * * * *

Applicants have made a good faith attempt to place this Application in condition for allowance. Favorable action is requested. If there is any further point requiring attention

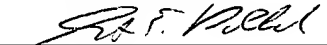
prior to allowance, the Examiner is asked to contact Applicants' counsel at (646) 265-1468.

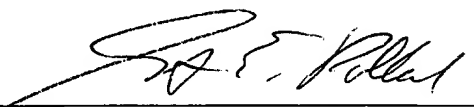
Respectfully submitted,

Dated: June 20, 2005

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail, in an envelope with sufficient postage addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

on June 20, 2005
Name Grant E. Pollack


Signature


Grant E. Pollack, Esq.
Registration No. 34,097
POLLACK, P.C.
The Chrysler Building
132 East 43rd Street, Suite 760
New York, New York 10017
(646) 265-1468

Attorney for Applicants